

SECTION BY SECTION ANALYSIS

Section 1. Short Title

Section 1 provides that the short title of the Act is the "Digital Telephony and Communications Privacy Improvement Act of 1994."

Section 2. Purpose

Section 2 states the purpose of the Act is to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information (e.g., dialed number information) pursuant to the Federal and state electronic surveillance and pen register and trap and trace statutes. An effective electronic surveillance capability is essential to Federal, state, and local agencies so that they can secure the public safety, effectively enforce the law, and maintain the national security. Without clarification of the increased responsibilities of the telecommunications industry to assist and cooperate, this critical investigative technique will be eroded, if not precluded, by the advances in telecommunications technology.

The statutory requirement for common carriers and others to provide needed assistance to law enforcement agencies in the execution of electronic surveillance court orders and lawful authorizations is a long-standing one. Since 1970, the assistance of common carriers and others has been mandated. In a 1970 amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), Congress enacted a provision specifying that a "communication common carrier [common carrier], landlord, custodian, or other person shall furnish [the government applicant for court-ordered electronic surveillance] forthwith all information, facilities, and technical assistance necessary to accomplish the interception" In return for providing the information, facilities, and technical assistance, the assistance provider is required to be compensated by the applicant for reasonable expenses incurred in providing the assistance. See 18 U.S.C. 2518(4).

The foregoing "assistance" provision also has been incorporated in the Foreign Intelligence Surveillance Act of 1978 (FISA) (codified at 50 U.S.C. 1805(b)(2)(B)) and in the pen register/trap and trace provisions of the Electronic Communications Privacy Act of 1986 ("ECPA") (codified at 18 U.S.C. 3134(a), (b)).

The purpose of the legislation is to clarify and define the nature and extent of this responsibility which arises from the stark mandate of the foregoing laws.

In 1970, the telephone industry was monolithic, and the part of the telecommunications network where government effected electronic surveillance was relatively uncomplicated. Since that time, with the breakup of AT&T through divestiture, the entry of numerous new communications providers in the telecommunications marketplace, and the introduction of many new (and often proprietary) technologies, services, and features, the telecommunications networks have become more varied, advanced, and complicated. Though unintended, the complexities of the telecommunications networks create, and will continue to create, impediments to Federal, state, and local government agencies as they attempt to execute electronic surveillance and pen register and trap and trace court orders and authorizations.

With the passage of the ECPA amendments to Title III, electronic communications have received statutory privacy protection as well, and the term common carrier has been replaced with the broader terminology of provider of wire or electronic communication service. However, intercepting voice communications and acquiring the attendant dialing information remain of the greatest importance to government agencies; and the principal area where technological impediments have been encountered is within the networks of wireline and cellular common carriers.

Solutions have not always been readily available for existing problems, and they may not be for the future problems that are foreseen in the emerging technologies, services, and features. Such solutions also take time and may require significant "capital" outlays. As a result, industry and government agencies have been uncertain as to the nature and extent of the foregoing "assistance" provision. In particular, key questions exist in terms of who is responsible for efforts to remove the impediments; how quickly the impediments should be removed; what the consequences are, if any, for not removing them in a timely fashion; and who is responsible for paying the costs.

Because of concerns about compromising investigations, harming law enforcement and common carrier relationships, and due to the prospect of substantial delays, government agencies have been reluctant to pursue contempt or other legal remedies to resolve this issue. Also, because of the variety of technological impediments and the differences in levels of effort required to remove them, the government has been concerned that a particular judicial ruling may have only limited precedential value. Consequently, as things now stand, common carriers and other communications service providers ultimately decide what they will do to remove technological impediments, and when. When carriers

and providers have acted, it frequently has taken months, and in some instances years, for ad hoc technical solutions to be developed, and the rate and breadth of their deployment have been uncertain. Thus, since the mid-1980s, technological impediments have frustrated, in whole or in part, the execution of a number of court orders for electronic surveillance, pen registers, or trap and traces, while the means of approaching and resolving the overall problem of the negative impacts of advanced telecommunications technology on electronic surveillance has eluded government and industry.

It has been observed that while it may be somewhat difficult and expensive to remove some existing impediments forthwith, that where new, advanced services and features are still under development or where upgrades are being prepared that technological solutions could be applied with significantly less difficulty and expense. Additionally, some common carriers, especially those who only more recently have entered the marketplace, have noted that they are not familiar with all of the electronic surveillance requirements of government agencies. Finally, some common carriers have stated that they rely on certain support service providers and equipment manufacturers to provide telecommunications service, and that without the help of those entities they may be unable to make the modifications required to remove the impediments and meet the requirements of government agencies.

Although Government and industry have made efforts to resolve this problem, after several years of discussion and consultation, the basic concerns and issues remain: what are the requirements of government agencies in this area; who is responsible for removing the impediments that impact on these requirements; how quickly must these requirements be met; what are the consequences, if any, for not meeting them on a timely basis; and who is responsible for paying the costs. This legislation addresses and resolves these concerns and issues.

The "Purpose" section also indicates that, excepting section 4, the legislation is not intended to alter any provision in the Federal electronic surveillance, pen register, or trap and trace statutes, or those of any state or other jurisdiction, such as those regarding the authority to intercept communications or install or use pen register and trap and trace devices; the current duty to provide assistance and receive payment therefor; causes of action; civil liability; or good faith defenses. The underlying purpose of the legislation is to clarify and define the responsibilities of common carriers such that government agencies can maintain their ability to properly and effectively execute electronic surveillance-related court orders and lawful authorizations.

An additional purpose to the Act, as set forth in section 4, is to improve communications privacy protection for users of cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications.

Section 3. New Section

Chapter 109 of title 18, U.S.C. is amended by adding a new section, section 2237, entitled: "Common carrier assistance to government agencies." Amendment of this chapter is made in order to avoid having to amend three separate, yet interrelated, Federal statutory regimes: Title III (18 U.S.C. 2510 et seq.); FISA (50 U.S.C. 1801 et seq.); and the pen register and trap and trace provisions of the ECPA (18 U.S.C. 3121 et seq.).

Common carrier assistance:

3a. Assistance requirements

Section 3(a) sets forth the requirements of government agencies when conducting electronic surveillance and pen register and trap and trace investigations. These requirements, which are generic in nature, were developed by the FBI and include input from representatives of various Federal, state, and local law enforcement agencies that utilize electronic surveillance extensively. These requirements relate to the capabilities needed to accomplish effectively the interception of communications and the acquisition of call setup information. The Government intentionally has eschewed setting any technical standards because it does not desire to "dictate" particular technological solutions. Further, owing to the diversity (and often proprietary nature) of each carrier's network and the variations in approaches that can be taken to achieve compliance, it is the Government's position that each common carrier is best positioned and qualified to determine how it will meet the requirements in the most cost-effective way.

Although the requirements set forth in section 3(a) constitute the first legislative listing of the government's requirements, the FBI states that for many years most, if not all, of these requirements have been known to the security offices of the major local exchange carriers, interexchange carriers, and cellular carriers. (Security offices usually are designated by common carriers to receive service of the court orders and authorizations and to provide law enforcement agencies with the information and assistance required to execute the court orders and authorizations.)

The legislation requires common carriers to provide "forthwith" the capability and capacity necessary to permit the government to conduct electronic surveillance, pen register, and trap and trace investigations effectively. The requirement of providing assistance "forthwith" is not new. It is found in the current language of 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805 (b)(2)(B). The language concerning capability and capacity is included to underscore the need for a common carrier to afford not only an ability to effect the interception of communications and the acquisition of call setup information (which includes dialed number information) but also the ability to accommodate without delay all court orders and authorizations for electronic surveillance, pen registers, and trap and traces that may be served on such common carrier by the various Federal, state, and local government agencies.

Within section 3(a)(1), it is stated that the foregoing capability and capacity must accommodate the "expeditious" and "simultaneous" execution of all court orders and authorizations. Frequently, it is essential to implement the interception of communications or acquire dialed number information expeditiously in order to obtain information critical to saving lives, making arrests, and seizing evidence and contraband, such as drugs, illegal weapons, bombs and other explosive devices.

The capability and capacity requirement is also very important inasmuch as a number of government agencies must be able to execute a number of court orders and authorizations simultaneously. The FBI states that over the past decade a number of court orders and authorizations were not fully executed, or were not even sought, because of certain technological impediments and capacity shortfalls, such as insufficient "port" capacity in the cellular mobile switching offices (MSOs). At any particular time a number of Federal, state, and local government agencies may be competing to execute electronic surveillance and pen register court orders regarding certain telecommunication facilities, the access point for which is of limited capacity. Inasmuch as communications interceptions and dialed number acquisitions increasingly will be activated from within common carrier premises, including switching offices, it is critical that there be sufficient capacity to accommodate completely the concomitant needs of all government agencies.

As discussed below with regard to section 3(g), since common carriers' technological responses to the requirements will vary by common carrier and by the technology being addressed, and because historically each carrier has been subject to varied numeric demands in terms of court orders or authorizations, the Government intends to consult with common carriers and telecommunications industry representatives in a number of areas, such as in the area of capacity, in order to assist in facilitating

proper sizing approaches and cost-effective compliance. Further, it is expected that most common carriers can ensure compliance in the future and gauge the future demands of government agencies by reviewing their records as to the numbers of, and trends in, current and past court orders and authorizations and extrapolating therefrom the sizing required to meet future demands. Finally, the increasing availability of "modular" and incremental technical approaches will allow common carriers to respond flexibly throughout their networks to the demands of government agencies in a cost-effective manner.

Section 3(a)(2) specifies that common carrier networks must afford government agencies an ability to intercept communications and acquire call setup information "concurrent" with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or authorization, to the exclusion of communications or information concerning any other subscriber, and without regard to the mobile nature of the subject subscriber's facility or service or the use by that subscriber of any custom features or services offered by the common carrier.

It is important that government agencies can intercept communications concurrent with the transmission of the original communication. Further, the associated requirement of being able to acquire call setup information concurrent with the subject transmission also is essential. For example, it is critical for government agencies to be able to intercept communications as they occur so they can respond immediately to life-threatening circumstances and react promptly and effectively to criminal activity in terms of making needed arrests, seizing evidence, and interdicting contraband, such as drugs, illegal weapons, bombs and other explosive devices.

The separation of signaling transmission paths from communications paths also can impede government agencies who must be able to associate the intercepted communication with the calling or called party. Aside from the negative evidentiary impact caused, this circumstance can hamper government agencies in their efforts to effectively "minimize" the monitoring and recording of non-criminal communications. Consequently, there is a requirement that common carriers can assure that call setup information will be available "concurrent with the transmission of the communication" that is the subject of the court order or authorization.

Owing to the varying availability of contemporaneous call setup information, the definition of "concurrent with the transmission of the communication" found in section 3(i)(6) specifies that the "concurrence" requirement is satisfied if such information can be acquired by government agencies either before, during, or immediately after the transmission of the communi-

cation. It is the clear preference of government agencies that common carriers will attempt to afford the ability to acquire this information before the transmission of the communication whenever reasonably feasible. Similarly, because of the difficulty of intercepting certain "electronic communications" concurrent with their transmission, the foregoing definition states that providing government agencies an ability to intercept such information at the conclusion of the transmission will satisfy the requirement.

The requirement that government agencies will have the ability to isolate the communications and call setup information of the subjects of electronic surveillance to the exclusion of the communications and call setup information of other subscribers is a basic and a long-standing one. Government agencies do not want to be faced with the prospect of having to "sort through" a tangle of communications which include those of innocent individuals who have the misfortune of having their communications "bundled" or otherwise commingled with those of the interception subject in the telecommunication transmission process. This requirement is being challenged by the increased use of digital transport, multiplexing, and fiber optics closer to the premises of the interception subject. Hence, common carriers must assure that there are means to access and isolate communications and call setup information, yet in a fashion that does not compromise the interception or acquisition effort.

The increasingly mobile nature of telecommunications facilities and service also has created impediments to the effective execution of electronic surveillance. With today's cellular telephony, communications can be "handed off" within and between networks and can be routed about such that they bypass interception access points, even when they are established within the premises of a cellular common carrier. It is believed that the communication interception and call setup information acquisition requirements of government agencies can be met by common carriers affording mobile service by drawing upon existing technologies and programming and routing capabilities and by coordinating efforts with other mobile carriers. This same requirement also has application to other mobile features and services which permit subscribers to program or otherwise direct communications to any facility designated by the subscriber (e.g., "follow me service"), as well as to the emerging mobile services encompassed in personal communications services (PCS) and other radio frequency-based mobile communications services.

Section 3(a)(2) specifies that the communication interception and call setup information acquisition requirement includes an ability to obtain such communications and information notwithstanding the use by the subject subscriber of any telecommunications custom "features" offered by the common carrier. The most notable feature impediment to effective electronic surveil-

lance is "call forwarding." This feature permits a subscriber, whose telecommunications facility (and telephone number) is the subject of a court order or authorization, to redirect in-coming calls from that facility to other facilities. Such call redirection can be accomplished according to established programs or even randomly and dynamically. In the past, government agencies frequently have proceeded by securing additional court orders for those new facilities to which the calls have been "forwarded" or redirected by the subject subscriber of the court order or authorization. This circumstance has resulted in government agencies having to obtain more court orders or authorizations than typically would have been required; in criminal communications escaping timely interception; and, in some instances, in additional households unnecessarily becoming targets of electronic surveillance.

Section 3(a)(3) includes the requirement that there be an ability to intercept the content of communications and acquire call setup information unobtrusively and with a minimum of interference with any subscriber's telecommunications service. This language mirrors language currently found in 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B), and it is intended to prevent subjects of electronic surveillance and pen register and trap and trace investigations and others from detecting the surveillance effort.

Section 3(a)(4) contains the requirement that, once intercepted or acquired, the government agency would be able to receive the communication or call setup information in a generally available format at a location identified by the government agency distant from the subject's facility, from the interception or acquisition access point, and from the premises of the common carrier. This requirement is not new and is intended to maintain the current ability of government agencies to monitor, record, minimize, and otherwise properly administrate electronic surveillance and pen register and trap and trace investigations. This requirement is fundamentally important, since without it the safety of law enforcement officers and government employees would be put at risk, the interception or acquisition effort easily could be compromised through detection, and the effective execution of the surveillance search would be significantly disrupted.

Currently, once access has been obtained within the local loop or the common carrier's central office facilities, the communications and call setup information are transmitted back to the law enforcement agency's facility or monitoring plant, usually within the agency's office. The transmission most frequently occurs via line facilities provided by the common carrier.

The language which states that the communications and call setup information are to be received in a generally available format is intended to make clear that government agencies do

not expect common carriers to translate digital transmissions to analog, etc. before affording transmission to them. Rather, it is expected that a common carrier would utilize a transmission format that was consistent with that of the communication being intercepted or acquired at the time of access, such as analog voice channel on a local loop, D4 formatted T-1 circuit, ISDN Primary Rate Interface circuit, etc. On the other hand, government agencies understand that they, not the common carriers, are responsible for processing the communications intercepted and the call setup information acquired.

Section 3(a)(4) also indicates that in some emergency or exigent circumstances that a government agency by necessity may have to access and monitor communications or dialed number information on the common carrier's premises. Government agencies understand that common carriers are not desirous of having government personnel carry out all aspects of a surveillance on common carrier premises, and it is understood that the government's presence in common carrier premises should only occur in emergency or exigent circumstances. Also, government agencies are not expecting common carrier personnel to assist in the monitoring aspects of executing a court order or authorization.

Section 3(b) specifies that government agencies shall notify common carriers of any wire or electronic interceptions or any call setup acquisitions that are to be effected within the premises of such common carrier pursuant to court order or authorization. Common carriers are required to designate individuals to activate such interceptions or acquisitions. These individuals are required to be available at all times to activate the interceptions or acquisitions. The requirement can be met by such individuals being "on call," in order to promptly respond to governmental needs as necessary. The requirement does not mean that the designated individuals actually must be on the premises at all times or that 24 hour-a-day work shifts must be established. Such interceptions or acquisitions may be activated only by the affirmative intervention of such individuals.

This provision recognizes that the access point for intercepting communications and acquiring call setup information increasingly will originate within common carrier premises. Such premises include buildings, switching offices and facilities, and network elements (e.g., signaling transfer points) maintained by the common carriers. Since it is important that these facilities, as well as the entire telecommunications network, remain secure, it is a requirement that all such access be initiated directly only by individuals designated by the common carrier.

Government agencies are not seeking the authority or ability to remotely activate interceptions within the premises of a common carrier in a fashion that bypasses personnel designated by common carrier. All executions of court orders or authoriza-

tions which require access to the switching facilities or other premises will be made through the individuals authorized and designated by the common carrier. Activation of interceptions or acquisitions originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the common carrier, depending upon the amount of assistance the government requires.

Section 3(c) states that to the extent common carriers providing service within the United States currently cannot fulfil the requirements set forth in subsection (a), they shall fulfil such requirements within three years from the date of enactment of the Act. This section makes clear that the focus of compliance is on common carriers within whose networks most of the electronic surveillance occurs.

Nearly all wireline and wireless voice communications are provided by local exchange carriers, interexchange carriers (and increasingly by service "resellers" and competitive access providers (CAPS)), and by cellular carriers (and soon by providers of Personal Communications Services (PCS) and satellite-based mobile communications providers). These entities are common carriers, and historically they have been subject to regulation. Since most electronic surveillance is effected within the networks of common carriers, the coverage has been scaled to focus only on those service providers within whose networks the core technological problems exist.

Although certain categories of electronic communication service providers (e.g., PBX and computer network operators) who currently have assistance responsibilities under Federal and state laws are excluded from the provisions of this legislation, nevertheless it is expected that such providers will continue to fulfil their statutory responsibilities and undertake voluntarily to accommodate the electronic surveillance needs of government. If significant technological impediments arise within their networks in the future due to inattention to government requirements or due to inaction in addressing them, consideration would have to be given to seeking expansion in the coverage of the instant legislation to include such entities.

The language of the section is also intended to indicate that common carriers still must fulfil their assistance responsibilities under 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B) by furnishing requested information, facilities, and technical assistance, to the extent possible, during the three year grace period set for compliance. There should be no relaxation in common carrier efforts to assist government agencies in effectively executing court orders and authorizations.

Some common carriers, such as "resellers" and competitive access providers (CAPS), either may not own any equipment or

facilities or the equipment or facilities they own may be such that they are not capable of effecting interceptions or acquisitions under this Act. In such cases, it is expected that such service entities would rely on the compliance of the common carrier whose facilities they lease, etc., and that they likely would seek from such common carrier legal assurances that compliance will be achieved within the statutory compliance period or that such common carrier would indemnify them for any liability or penalty they may incur if compliance is not met. If a common carrier leases a portion of its switching or other network facilities to an end user and such facilities are not under the carrier's control, then the carrier shall not be obligated to make that portion compliant as long as it remains beyond the common carrier's control.

The date for common carrier compliance is set at within three years from the date of enactment of the Act. The Government believes that this is a reasonable period within which the needed technological solutions can be identified, tested, and deployed within the networks of common carriers. As discussed below, common carriers receive important assistance and cooperation of equipment manufacturers and common carrier support service providers so that timely compliance can be achieved.

The coverage of compliance includes needed modifications to existing systems and networks (embedded base) as well as to future systems and networks (those fielded after the three year compliance period).

Section 3(d) provides that common carriers shall consult in a timely fashion with providers of common carrier support services and telecommunications equipment manufacturers so that any needed modifications to services and equipment, including hardware and software, can be made, and thus help to ensure common carrier compliance within three years. This section further specifies that a provider of common carrier support services and a telecommunications equipment manufacturer shall make available to a common carrier on a timely and priority basis, at a reasonable and cost-effective charge, any support services or equipment required so as to permit compliance with the provisions of the Act. The responsibilities of common carrier support service providers and equipment manufacturers are added to the legislation to indicate that they have an important role in ensuring that court orders and authorizations are not frustrated.

Assistance and cooperation from support service providers and equipment manufacturers are increasingly important, as services and equipment become more sophisticated and as common carriers rely on "outside" companies to provide them with these components. Although the direct burden of compliance falls on common carriers, nevertheless statutory responsibilities are conferred upon these support service providers and equipment

manufacturers without whose help the common carriers likely could not comply. One of the major objections to the compliance date and attendant penalty provisions raised in the past by representatives of the Regional Bell Operating Companies (RBOCs) was the concern that local exchange carriers must rely on equipment manufacturers and others in order to meet many of the requirements.

Under provisions of the Modified Final Judgment (MFJ) of the consent decree regarding the Government's antitrust case against AT&T, local exchange carriers are precluded from engaging in telecommunications equipment manufacturing. However, a Department of Justice memorandum concludes that Judge Greene's order would not be an impediment to a common carrier's effecting limited, noncommercial modifications to network facilities, services, or equipment, the sole purpose of which would be to prevent the frustration of statutorily-based court orders and authorizations designed to ensure effective law enforcement, the public safety, and the national security.

Section 3(e) states that the Attorney General of the United States shall have the authority to enforce the provisions of subsections (a), (b), (c), and (d) of section 3. In order to avoid disparate enforcement actions throughout the country in ways that could be burdensome for common carriers, the responsibility for enforcing these provisions is vested in the Attorney General of the United States through the Department of Justice and the Offices of the various United States Attorneys.

In particular, the Attorney General is specifically given the authority to apply to an appropriate United States District Court for an order restraining or enjoining the provision of service by any common carrier who violates the foregoing subsections of section 3. Similarly, to ensure common carrier compliance, the Attorney General may apply for an order, such as a writ of mandamus, which mandates the cooperation of a provider of common carrier support services or a telecommunications equipment manufacturer pursuant to the provisions in subsection (d). The intent is that there be no excuse offered by common carriers that they cannot comply because of unresponsiveness on the part of such support service providers and equipment manufacturers. The Federal district courts are specifically given jurisdiction to issue such orders. Additionally, the Attorney General may request the Federal Communications Commission (FCC) to assist in enforcing provisions of the Act. This provision recognizes the wide-ranging authority of the FCC over common carriers and others in the telecommunications industry.

Section 3(f) specifies that any common carrier that violates section 3(a) shall be subject to a civil penalty of \$10,000 per day for each day in violation. The Attorney General is authorized to file a civil action to collect, and the Federal

district courts have jurisdiction to impose, such fines. The FCC may also impose regulatory sanctions or fines authorized by law.

Section 3(g) provides that the Attorney General is encouraged to consult with the FCC and common carrier representatives and to utilize common carrier standards bodies, associations, and other such organizations to discuss details of the requirements, such as those related to capacity, in order to facilitate compliance with the provisions of the Act. This subsection evidences an intention on the part of Government to help common carriers achieve compliance with as little difficulty as possible, and in the most cost-effective way possible. Through detailed discussions, narrow and technical questions from common carriers can be answered and other concerns addressed.

Such fora also may act as potential clearinghouses for promising, cost-effective technological approaches and solutions, which would likely reduce costly and duplicative independent efforts on the part of each common carrier. The FBI and other law enforcement agencies have been meeting with industry (largely common carrier) technical committees for nearly two years in this regard, currently under the auspices of the Alliance for Telecommunications Industry Solutions' Electronic Communications Service Provider Committee (ECSPC). However, because of the voluntary basis and elective nature of participation, in and commitment to this body, its lack of authority to require the implementation of solutions or to assign funding responsibility, and given that there is no clear legal mandate to fulfill government's requirements on a timely basis, these committees have not been effective to date in engendering the development, let alone the implementation, of the required solutions. With legislation mandating future compliance and addressing funding concerns, it is reasonable to assume that common carriers and others will utilize such committees in a more meaningful and beneficial fashion.

Section 3(h) states that the Federal Government shall pay common carriers for reasonable and cost-effective charges directly associated with the modifications required to assure common carrier compliance with the requirements of this Act which are incurred within the three year period set for compliance.

The Federal Government has concluded that it should compensate common carriers for reasonable and cost-effective charges associated with devising and implementing the modifications required which remove the technological impediments and assure common carrier compliance with the government's requirements established in section 3(a). The remuneration covers charges incurred within the three year period set for compliance with regard to certain interim solutions to remove the impediments that most concern the Government; for the cost of modifying existing networks, services, facilities, and features; and for research and development and testing efforts associated with

making future networks, services, and features compliant with the government's requirements. Once solutions have been identified, it is expected that they would be incorporated into successive generations of service and, where feasible, into new services without additional charge to the Government.

Section 3(i) sets forth definitions for sections 1-3 of the Act. The term "common carrier" means any person or entity engaged as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service or interconnected service, as defined in section 6002(b) of Public Law 103-66. This definition encompasses such service providers as local exchange carriers, interexchange carriers, service "resellers," competitive access providers (CAPS), cellular carriers, personal communications services (PCS), satellite-based service providers, and any other common carrier who offers wireline or wireless service to the general public.

The term "provider of common carrier support services" means any person or entity who provides services to a common carrier that are integral to processing, directing, forwarding or completing telephone calls or electronic communication transmissions. There are currently over one hundred such support service providers that provide common carriers with specialized support services.

The terms "wire communication" and "electronic communication" have the same meaning as set forth at 18 U.S.C. 2510(1) and 2510(12), respectively, under Title III, as amended by the ECPA.

The term "intercept" has the same meaning as set forth at 18 U.S.C. 2510(4), except that with regard to a common carrier's transmission of a communication encrypted by a subscriber, the common carrier shall not be responsible for ensuring the government agency's ability to acquire the plaintext of the communications content, unless the encryption was provided by the common carrier and the common carrier possesses the information necessary to decrypt the communication. The term "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication...." The term "contents" includes "any information concerning the substance, purport, or meaning of [a]... communication." 18 U.S.C. 2510(8). The language in the definition of "intercept," as used in this legislation, is intended to clarify that a common carrier has no obligation to decrypt communications that have been encrypted by the subscriber, such that the conversation or data transmission can immediately be understood by the government, unless the encryption was provided by the common carrier and the carrier possesses the information necessary to decrypt the communication.

The term "concurrent with the transmission of the communication" means contemporaneous with the transmission of the communication, but it also includes, with regard to electronic communications, the ability of the government to acquire such communications at the conclusion of the transmission, and, with regard to call setup information, the ability to acquire such information either before, during, or immediately after the transmission of the communication.

The definition of "concurrent with the transmission of the communication" found in section 3(i)(6), is somewhat broader than term might imply on its face. The definition was broadened due to the varying feasibility of effectively intercepting electronic communications contemporaneously and the varying availability of call setup information contemporaneous with the transmission of the communication with which it is associated. Because of the difficulty of intercepting certain electronic communications concurrent with their transmission, the foregoing definition states that providing an ability for government agencies to intercept such information at the conclusion of the transmission will satisfy the requirement. The definition also specifies, with regard to call setup information that the "concurrency" requirement is satisfied if such information can be acquired by government agencies either before, during, or immediately after the transmission of the communication. It is the clear preference of government agencies that common carriers will attempt to assure an ability to acquire this information before the transmission of the communication whenever reasonably feasible.

The term "call setup information" means the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunications system dialing or calling features or services. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted, or caused to be transmitted. In pen register investigations, these are the pulses, tones, or messages which identify the numbers dialed from the facility that is the subject of the court order or authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization.

With regard to electronic communications, the information is that generated during the establishment of communications or the transmission of a protocol data unit, such as a datagram, that identifies the origin and destination of the

communication. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as the header of a frame or packet.

The call setup information also encompasses numbers identified incidental to calls where calling features or services are used.

The term "government" means the Government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance.

Section 4. Communications Privacy Improvement and Monitoring Clarification.

Section 4 includes several amendments to Chapter 119, United States Code, which includes Title III, with regard to communications privacy improvements and clarifications concerning monitoring of electronic communications.

In section 4, amendments are made to the definitions found in 18 U.S.C. 2510(1) and (12). The purpose of the amending language is to provide communications privacy protection to cordless telephone communication transmissions occurring in the radio link between the telephone handset and base station.

Because of the ease with which communications occurring in the radio portion of cordless telephone transmissions could be overheard through the use of commercial radio receivers, scanners, and similar cordless telephones operating in the same area, Congress chose not to confer statutory privacy protection upon the radio portion of cordless telephone communications or to criminalize the interception of same in the 1986 ECPA amendments to Title III. However, since then, advances in cordless telephony have resulted in the mass-marketing of various types of cordless telephones, many of which are considerably more difficult to intercept than the earlier models. Because newer versions and types of cordless telephones incorporate features and technology that typically afford greater security to the user, there now exists a basis for providing full statutory privacy protection to cordless telephones. Even absent the prior statutory privacy protection, the view that certain cordless telephone users nonetheless retain Fourth Amendment privacy protection under the "reasonable expectation of privacy" criteria has been asserted. See United States v. Smith, 978 F.2d 171, 176 (5th Cir. 1992). This amendment now confers the same communications privacy protection for the millions of cordless telephone users as is currently afforded to cellular telephone users.

The penalty provisions for intercepting cordless telephones are also made consistent with those for intercepting cellular telephones, by the amendments to 18 U.S.C. 2511(4)(b)(i) and (ii) set forth in this section.

Section 4 also includes language which amends 18 U.S.C. 2510(16), communications deemed to be "readily accessible to the general public" with regard to radio communications, and the exceptions thereto. The excepted categories currently covered under section 2510(16)(A)-(E) enjoy privacy protection because they usually are not susceptible to interception by the general public. Added to these categories is the new category of "electronic communication." The intention is to provide clarification that there is protection for all forms of electronic communication, including data, even when they may be transmitted by radio.

Section 4 also amends the penalty provisions set forth in 18 U.S.C. 2511(4)(b) by adding language that specifies a similar penalty for intercepting communications "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication." The purpose of the amendment is to treat communications using such modulation techniques in the same fashion as those where encryption has been employed to secure communications privacy.

Finally, section 4 amends 18 U.S.C. 2511(2)(a)(i) by clarifying that it is not unlawful for a switchboard operator, officer, employee, or agent of a wire or electronic communication service to intercept, disclose, or use an "electronic communication," in the same fashion as a wire communication, in the normal course of his employment while engaged in any activity which is necessary incident to the rendition of his service or to the protection of the rights or property of the provider of the service. This technical correction is designed to put the handling of electronic and wire communications on the same footing.

Exhibit 2

ICC Comments

FCC No. RM 10865

04/12/2004

Digital Telephony



*A legislative proposal to ensure that law enforcement can continue to
protect the American public from criminal activity.*

DIGITAL TELEPHONY SUMMARY OF ISSUES

- The Nation's various telecommunications systems are often used in the furtherance of serious and sometimes violent criminal activities including illegal drug trafficking, organized crime, terrorism, kidnaping and extortion. One of the most important and effective tools in the investigation of these crimes by Federal, state and local law enforcement agencies is the court-authorized interception of communications (wiretaps).
- The telecommunications industry, which has relied on the same analog technology for approximately 50 years, is now rapidly moving to more advanced telecommunications systems and fundamentally different technology, e.g., personal communication networks, advanced cellular, and integrated services digital networks. These new technologies have the capacity for high speed, simultaneous transmission of multiple, commingled communications.
- These advances in technology, and undoubtedly the future introduction of new technologies, will soon make it impossible for law enforcement agencies to effect lawful court orders to intercept electronic communications. In some cases, advanced cellular technology and new digital features have already frustrated orders, thereby allowing criminals to carry out serious criminal activity using the telecommunications systems without detection.
- These technologies inadvertently hamper the ability of law enforcement to investigate crimes and protect the public safety. This happened because the legitimate needs of law enforcement were not considered during the design and development phases of the systems. These new systems are unable to provide law enforcement with the content of communications by the target of the court-authorized electronic interception, to the exclusion of all other communications by persons not engaged in criminal conduct. This was not a problem with the old analog technology because every communication was distinct and identifiable and could be accessed at several points within the network. Without modifications to systems software and, in some cases, hardware, the telecommunications systems of this country will no longer be able to accommodate access by law enforcement to conduct electronic surveillance.
- Following discussions about this issue with the telecommunications industry, the Congress, the White House, and other Federal agencies; the Department of Justice and the FBI have proposed legislation which seeks to preserve the status quo, i.e., the current ability to

obtain a court-authorized warrant and, with assistance from the telephone companies, intercept specific communications that are in the furtherance of criminal conduct. This proposal relies on the telecommunications industry to develop technical solutions which are both cost effective and that will ensure that telecommunications technology continues to be designed, manufactured, and deployed in a competitive fashion that still meets the needs of law enforcement.

- * The proposal, if enacted, simply requires the telephone companies, when served with a court order, to be able to identify and provide the entire content of specific telephone conversations to the exclusion of all others, regardless of the technology involved. This is what the telephone companies do now in the analog format but cannot do in the digital format absent some modifications.
- * The legislative proposal also ensures that all providers of telecommunications services remain on the same competitive "level playing field" by requiring all telecommunications service providers ultimately to use systems that take into consideration both the legitimate need for law enforcement to access criminal conversations and the intense competitive demands of the market place.
- In 1968, Congress carefully considered and passed the Omnibus Crime Control and Safe Streets Act which laid out a meticulous procedure by which law enforcement can obtain judicial authorization to conduct electronic surveillance. This law was enacted after Congress exhaustively debated the Government's need to effectively address serious and often violent criminal conduct against an individual's right to privacy. Nothing in this proposal seeks to change or enhance this authority or procedure. The 1968 law requires the telecommunications industry to provide the "technical assistance necessary to accomplish the interception." What has been proposed is legislation clarifying the duties of the telecommunications industry in responding to court orders and assisting law enforcement in the face of advances in digital telephony technology.
- Thirty-seven states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation authorizing their State and local law enforcement agencies to conduct court authorized electronic surveillance in criminal investigations. Approximately 60 percent of the court-authorized criminal wiretaps conducted annually in this country are by state and local law enforcement agencies. These also will not be possible absent a viable solution.

**DIGITAL TELEPHONY
SUMMARY OF LEGISLATIVE PROPOSAL**

The purpose of this proposal is to clarify the responsibilities of the providers of electronic communication services when providing law enforcement with the "technical assistance necessary to accomplish the interception," required by Title 18, U.S.C., Section 2518(4) and Title 18, U.S.C., Section 3124(a)(b). This clarification is needed to ensure that the Government's continued technical ability to conduct intercepts is not impeded by current or emerging telecommunications technology. Specifically, the new legislative proposal provides for the following:

1. Clearly establishes, as a matter of law, the responsibilities of electronic communication service providers and private branch exchange operators within the United States in providing the Government with the technical assistance necessary to conduct the lawful interceptions of communications. These include the ability to provide the Government with:

- The real time and identical communication signals as transmitted to or by the individual(s) named in the court order.
- Isolation of all communication signals and services directed to and/or from the subject of the intercept to the exclusion of all other users who are not the subject of the lawful interception.
- The intercepted communication signals provided by the telephone company to the Government at a monitoring facility that is remote from the target of the court order and not in the facility of the communications service provider.
- Without detection by the subject of the interception or any other subscriber.
- Without degradation or interruption of the subscriber's telecommunications service.

2. Providers of electronic communications services within the public switched network, such as local exchange carriers, interexchange carriers, cellular carriers, etc., shall ensure that their systems comply with these requirements within 18 months of enactment into law.

3. Private branch exchange operators shall ensure that their systems comply with these requirements within 3 years of enactment into law.

4. Provides the Attorney General with the authority to grant exceptions to these requirements as well as exceptions to the implementation deadlines. In considering any request for an exception, the Attorney General must consult with the Federal Communications Commission, the Small Business Administration, and the Department of Commerce.

5. Provides the Attorney General specific authority to seek civil penalties and injunctive relief to enforce the provisions of this law.



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 14, 1992

Honorable Dan Quayle
President of the Senate
Washington, D.C. 20510

Dear Mr. President:

Enclosed for referral to the appropriate committee or committees is a draft bill to clarify the responsibilities of electronic communication service (ECS) providers and private branch exchange (PBX) operators to assist the government to implement lawful court orders or authorizations to intercept wire and electronic communications. The draft bill does not change in any way any existing statutory authority to intercept wire or electronic communications. Nor does it diminish or otherwise affect existing sanctions against unauthorized interceptions. We have enclosed a section-by-section analysis that explains our proposal in greater detail.

By way of background, telecommunications systems and networks are often used to further organized crime, racketeering, extortion, kidnapping, espionage, terrorism, and trafficking in illegal drugs. Recent and continuing advances in technology by the telecommunications industry, however, have made it increasingly difficult for government agencies to implement lawful orders or authorizations to intercept wire and electronic communications. This, in turn, threatens the ability of the criminal law enforcement community to enforce the laws and protect the Nation's security.

This legislation addresses this serious problem in a simple, straightforward fashion. As a general matter, the draft bill clarifies minimum attributes for ECS providers and PBX operators to provide, within the United States, the capability and capacity for criminal law enforcement agencies to intercept electronic communications, when authorized by law. The proposal would establish an 18 to 36 month "window" for existing systems and operators to comply with six intercept attributes (e.g., that access to a communication must be provided concurrent with its transmission) that are set forth in the draft bill. The Attorney General also is authorized to make exceptions and grant waivers in appropriate cases.

Enactment of this legislation this year is essential if we are to ensure the continuing capability of the law enforcement community to combat large scale drug trafficking, organized crime, and other forms of serious criminal activity. I therefore urge its prompt consideration and speedy enactment.

The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the presentation of this legislative proposal, and that its enactment would be in accord with the program of the President.

Sincerely,

A handwritten signature in dark ink, appearing to read 'W. Lee Rawls', written in a cursive style.

W. Lee Rawls
Assistant Attorney General

Enclosures

102nd Congress
2nd Session

S. _____
[H.R. _____]

IN THE SENATE
[IN THE HOUSE OF REPRESENTATIVES]

M. _____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To ensure the continuing access of law enforcement to the content of wire and
electronic communications when authorized by law and for other purposes.

*Be it enacted by the Senate and the House of Representatives of the United States
of America in Congress assembled,*

1 SEC. 1. FINDINGS AND PURPOSES.

2 (a) The Congress finds:

3 (1) that telecommunications systems and networks are often used in the
4 furtherance of criminal activities including organized crime, racketeering,
5 extortion, kidnapping, espionage, terrorism, and trafficking in illegal drugs;

6 (2) that recent and continuing advances in telecommunications technology,
7 and the introduction of new technologies and transmission modes by the
8 telecommunications industry, have made it increasingly difficult for government
9 agencies to implement lawful orders or authorizations to intercept wire and
10 electronic communications and thus threaten the ability of such agencies
11 effectively to enforce the laws and protect the national security; and

1 (3) that without the assistance and cooperation of providers of electronic
2 communication services and private branch exchange operators, the introduction
3 of new technologies and transmission modes into telecommunications systems
4 without consideration and accommodation of the need of government agencies
5 lawfully to intercept wire and electronic communications would impede the ability
6 of such agencies effectively to carry out their responsibilities.

7 (b) The purpose of this Act is to clarify the responsibilities of providers of
8 electronic communication services and private branch exchange operators to provide
9 such assistance as necessary to ensure the ability of government agencies to
10 implement lawful court orders or authorizations to intercept wire and electronic
11 communications. Nothing in this Act is intended to expand or reduce the authority
12 of the government to lawfully intercept the content of communications. Nothing in
13 this Act is intended to ~~expand or reduce any criminal penalties~~ for unlawfully
14 intercepting the content of communications.

15 SEC. 2. (a) Providers of electronic communication services and private branch
16 exchange operators shall provide within the United States capability and capacity for
17 the government to intercept wire and electronic communications when authorized by
18 law:

19 (1) concurrent with the transmission of the communication to the recipient
20 of the communication;

21 (2) in the signal form transmitted by the electronic communication services
22 provider or private branch exchange operator that represents the content of the
23 communication between the subject of the intercept and any individual with whom
24 the subject is communicating, exclusive of any other signal representing the

1 content of the communication between any other subscribers or users of the
2 electronic communication services provider or private branch exchange operator,
3 and including information on the individual calls (including origin, destination and
4 other call set-up information), and services, systems, and features used by the
5 subject of the interception;

6 (3) notwithstanding the mobility of the subject of the intercept or the use
7 by the subject of the intercept of any features of the telecommunication system,
8 including, but not limited to, speed-dialing or call forwarding features;

9 (4) at a government monitoring facility remote from the target facility and
10 remote from the system of the electronic communication services provider or
11 private branch exchange operator;

12 (5) without detection by the subject of the intercept or any subscriber; and

13 (6) without degradation of any subscriber's telecommunications service.

14 (b) Providers of electronic communication services within the public switched
15 network, including local exchange carriers, cellular service providers, and interex-
16 change carriers, shall comply with subsection (a) of this section within eighteen
17 months from the date of enactment of this subsection.

18 (c) Providers of electronic communication services outside of the public switched
19 network, including private branch exchange operators, shall comply with subsection
20 (a) of this section within three years from the date of enactment of this subsection.

21 (d) The Attorney General, after consultation with the Department of Commerce,
22 the Small Business Administration and the Federal Communications Commission, as
23 appropriate, may except from the application of any part or all of subsections (a), (b)
24 and (c) of this section classes and types of providers of electronic communication

1 services and private branch exchange operators. The Attorney General may waive
2 the application of any part or all of subsections (a), (b) and (c) of this section at the
3 request of any provider of electronic communication services or private branch
4 exchange operator.

5 (e) The Attorney General shall have exclusive authority to enforce the provisions
6 of subsections (a), (b) and (c) of this section. The Attorney General may apply to
7 the appropriate United States District Court for an order restraining or enjoining any
8 violation of subsection (a), (b) or (c) of this section. The District Courts shall have
9 jurisdiction to restrain and enjoin violations of subsections (a) of this section.

10 (f) Any person who willfully violates any provision of subsection (a) of this
11 section shall be subject to a civil penalty of \$10,000 per day for each day in violation.
12 The Attorney General may file a civil action in the appropriate United States District
13 Court to collect, and the United States District Courts shall have jurisdiction to
14 impose, such fines.

15 (g) Definitions -- As used in subsections (a) through (f) of this section --

16 (1) 'provider of electronic communication service' or 'private branch
17 exchange operator' means any service or operator which provides to users thereof
18 the ability to send or receive wire or electronic communications, as those terms
19 are defined in subsections 2510(1) and 2510(12) of Title 18, United States Code,
20 respectively, but does not include the government of the United States or any
21 agency thereof;

22 (2) 'communication' means any wire or electronic communication, as
23 defined in subsections 2510(1) and 2510(12), of Title 18, United States Code;

1 (3) 'intercept' shall have the same meaning as set forth in section 2510(4)
2 of Title 18, United States Code; and

3 (4) 'government' means the Government of the United States and any
4 agency or instrumentality thereof, any state or political subdivision thereof, the
5 District of Columbia, and any commonwealth, territory or possession of the
6 United States.

•